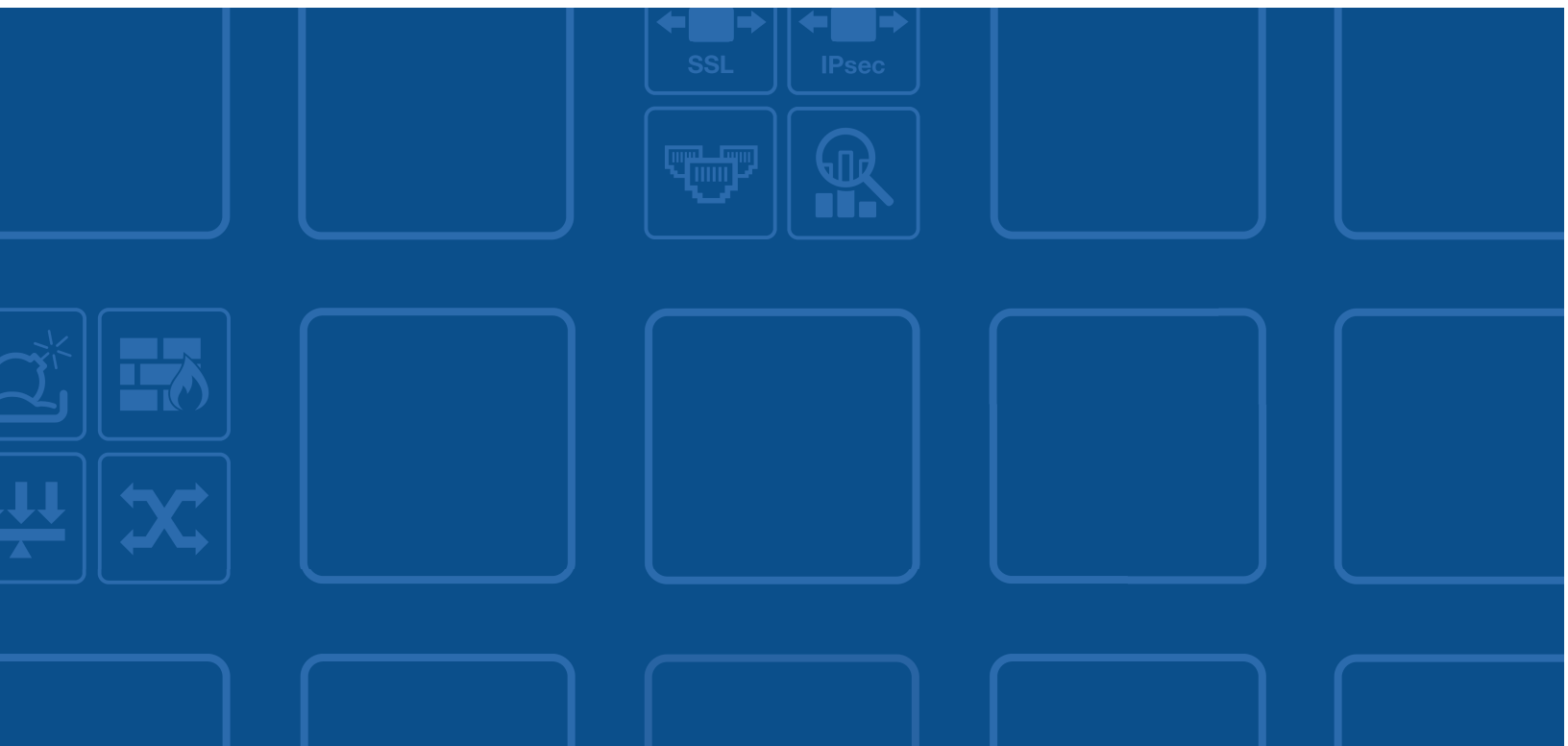
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.2.6



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

March 22, 2017

FortiOS 5.2.6 Release Notes

01-526-307845-20170322

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-01-29	Initial release.
2016-02-02	Added FGT-VM64-AWS/AWSONDEMAND build 8898 and FGT-VM64-AZURE build 5174 to Supported Models.
2016-02-24	Added Introduction > Last Release of Software section.
2016-03-04	Added RHEL 7.1/Ubuntu 12.04 and later to Product Integration and Support.
2017-03-22	Added note to *Known Issues > 273910*.

Introduction

This document provides the following information for FortiOS 5.2.6 build 0711:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.2.6 supports the following models.

FortiGate	FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-SFP, FG-60C-POE, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG- 111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-310B-DC, FG-311B, FG-400D, FG-500D, FG-620B, FG-620B-DC, FG- 621B, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-3950B, FG-3951B, FG-5001B, FG-5001C, FG-5001D, FG-5101C
FortiWiFi	FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-60D, FGR-100C
FortiGate VM	FG-VM32, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B
FortiOS Carrier	FCR-3950B and FCR-5001B FortiOS Carrier 5.2.6 images are delivered upon request and are not available on the customer support firmware download page. FortiOS Carrier firmware image file names begin with *FK*.

The following models are released on a special branch based off of FortiOS 5.2.6. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays the build number.

FGT-VM64-AWS /AWSONDEMAND	FGT-VM64-AWS/AWSONDEMAND is released on build 8898.
FGT-VM64-AZURE	FGT-VM64-AWSONDEMAND is released on build 5174.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 0711.

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0711-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0711-FORTINET.out image.

Last Release of Software

Due to the device flash size limitations, the following FortiGate models' last release of software will be FortiOS version 5.2.5. It is noted that these devices already have entered into their End-of-Life Cycle. Further details and exact dates can be found on the Fortinet Customer Support portal:

Affected Products:

- FortiGate FG-3016B
- FortiGate FG-3810A
- FortiGate FG-5001A SW & DW
- FortiCarrier FK-3810A
- FortiCarrier FK-5001A SW & DW

What's new in FortiOS 5.2.6

For a list of new features and enhancements that have been made in FortiOS 5.2.6 see the *What's New for FortiOS* 5.2.6 document available in the Fortinet Document Library.

The following enhancements have been made in FortiOS 5.2.6:

- Bug fixes
- New FortiGate models support

Special Notices

Compatibility with FortiOS versions

The following units have a new WiFi module built-in that is not compatible with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FWF-60CX-ADSL	PN: 8918-04 and later

The following units have a memory compatibility issue with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FG-600C	PN: 8908-08 and later
FG-600C-DC	PN: 10743-08 and later
FG-600C-LENC	PN: 11317-07 and later

Router Prefix Sanity Check

Prior to FortiOS 5.2.4 under the config router prefix table, if there are any `le` and `ge` settings that have the same prefix length as the prefix, you may lose the prefix rule after upgrading to FortiOS 5.2.4 or later.

WAN Optimization in FortiOS 5.2.4

In FortiOS 5.2.4:

- If your FortiGate does not have a hard disk, WAN Optimization is not available.
- If your FortiGate has a hard disk, you can configure WAN Optimization from the CLI.
- If your FortiGate has two hard disks, you can configure WAN Optimization from the GUI.

See the FortiOS 5.2.4 Feature Platform Matrix to check the availability for your FortiGate model.

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate-92D High Availability in Interface Mode

The FortiGate-92D may fail to form an HA cluster and experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used has the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

Default log setting change

For FG-5000 blades and FG-3900 series, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports STAT disk, log disk is enabled by default.

FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from version 5.0.7 (B4625) to FortiOS version 5.2.3, you may experience a back-plane interface connection issue. This is due to a change to the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

FortiGate units running 5.2.6

FortiGate units running 5.2.6 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

Firewall services

Downgrading from 5.2.3 to 5.2.2 may cause the default protocol number in the firewall services to change. Double check your configuration after downgrading to 5.2.2.

FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

Upgrade Information

Upgrading from FortiOS 5.2.4 or later

FortiOS version 5.2.6 officially supports upgrade from version 5.2.4 or later.

Upgrading from FortiOS 5.0.11 or later

FortiOS version 5.2.6 officially supports upgrade from version 5.0.11 or later.

When upgrading from releases prior to 5.0.11, if the source version is 5.0.10 with a configured HA cluster, you must schedule a down time; disable an uninterruptible upgrade; perform the upgrade; then, enable it back.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.2 Supported Upgrade Paths

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.2.6 support

The following table lists 5.2.6 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 42 • Google Chrome version 46 • Apple Safari version 7.0 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Internet Explorer versions 8, 9, 10, and 11 • Mozilla Firefox version 27 • Apple Safari version 6.0 (For Mac OS X) • Google Chrome version 34 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	• 5.2.4 and later You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	• 5.2.0 and later • 5.0.7 and later You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.2.5 and later
FortiClient iOS	• 5.2.2 and later
FortiClient Android and FortiClient VPN Android	• 5.2.7 and later

FortiAP	• 5.2.5 and later • 5.0.10 You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.
FortiSwitch OS (FortiLink support)	• 3.3.0 and later Supported models: FSR112D-POE, FS108D-POE, FS224D-POE, FS124D, FS124D-POE, FS224D-FPOE • 3.2.0 and later Supported models: FS-108D-POE, FS-224D-POE, FSR-112D-POE • 3.0.1 and later Supported model: FS-224D-POE • 2.0.3 Supported models: FS-28C, FS-324B-POE, FS-348B, FS-448B
FortiSwitch-ATCA	• 5.0.3 and later Supported models: FS-5003A, FS-5003B
FortiController	• 5.2.0 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 2.1.0 • 1.4.0 and later • 1.3.0

Fortinet Single Sign-On (FSSO)	• 5.0 build 0244 (needed for FSSO agent support OU in group filters)
	  • Windows Server 2008 (64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	• 4.3 build 0164 (contact Support for download)
	  • Windows Server 2003 R2 (32-bit and 64-bit)
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard Edition
	  • Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExplorer	• 2.6 build 1083 and later. Some FortiGate models may be supported on specific FortiExplorer versions.
FortiExplorer iOS	• 1.0.6 build 0130 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 2.0.0 build 0003 • 1.0.0 build 0024
AV Engine	• 5.174
IPS Engine	• 3.086
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, and 2012 R2
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish (Spain)	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Microsoft Windows XP SP3 (32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2323
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2323
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2323

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit)	Microsoft Internet Explorer versions 9, 10 and 11 Mozilla Firefox version 33
Microsoft Windows 7 SP1 (64-bit)	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Microsoft Windows 8/8.1 (32bit/62bit)	Microsoft Internet Explorer versions 10 and 11 Mozilla Firefox 42
Mac OS 10.9	Safari 7
Linux CentOS version 5.6	Mozilla Firefox version 5.6
Linux Ubuntu version 12.0.4	Mozilla Firefox version 5.6

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center 8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved Issues

The following issues have been fixed in version 5.2.6. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
260838	TCP flow does not support `AV fail-open` in flow mode.

Firewall

Bug ID	Description
306415	The SSL traffic causes the proxyworker to stop working.
305877	DSCP value is modified in transparent mode on FortiGate-100D.
276452	`Firewall auth` does not work as expected when the `src interface` is in PPPoE.
303962	VIP IP unexpectedly responds to `fgfm` requests.
304566	When `ssl inspect`-all is set to `deep-inspection`, the proxyworker stops working.
280584	MAPI inspection (wad) drops DCE/RPC packets when there is no MAPI traffic.
297196	The `strict-file option` does not correctly parse file names.
287799	High CPU usage occurs while transferring large files over SMB.
284957	HIBUN file types are not recognized even in an archive mode.
298411	Kernel Panic occurs and stops working on FortiCarrier-5101C cluster.
298236	Some MasterCard numbers are not detected by DLP.

FortiCarrier

Bug ID	Description
293134	GTP inspection blocks IPv6 traffic for dual-stack host.

FortiController

Bug ID	Description
273592	`SALB confsync` does not synchronize to the master's config when a FortiController-5001C worker blade is newly added.

FortiGate-3700D

Bug ID	Description
279273	GRE tunnel on NPU VDOM link interface is notable to pass traffic when offload is enabled.

FSSO

Bug ID	Description
285625	`SSO_Guest` users may not be able to pass the firewall after they agree to the disclaimer.

GUI

Bug ID	Description
276121	`Polling-id` used when adding new `adgrp` is not correct.
269123	Users cannot create address group containing URL Pattern (explicit proxy) objects.
274256	Received a `http 500 error` when trying to view a CA certificate.
286110	GUI shows different certificate name under the VPN SSL setting than in CLI.
274556	Drag and drop does not work for explicit proxy policies.
306595	DDNS page does not load properly for all interface types.
300372	GUI stops working once admin tries to login with two factor mail token.
295534	Policy list does not load properly when interfaces contains `&`.

High Availability

Bug ID	Description
289516	RTP sessions are deleted on HA slave when SIP session expires.
290250	After the hardware switch is deleted on FortiGate-90D, users are unable to establish HA when using an internal port.

Bug ID	Description
294950	`Radiusd` not able to synch with the DB with a secondary unit. The DB remains locked and users cannot authenticate.
299848	Remote and Wildcard admin are matched only versus one group on slave device.
298647	`npu_vlinks` receive the same `virtual-mac` in HA config.
291671	Radius(PAP) authentication does not work for slave FortiGate to Secondary Radius server.

IPS

Bug ID	Description
299585 306713	Some `NTurbo local mbuf` handling problems when processing IP fragmented packets.
295029	SynProxy DoS meter issue.
292175	DoS/Anomaly log has inaccurate service name.

IPSec

Bug ID	Description
269123	Traffic from IPSEC tunnel to IPSEC tunnel is not accelerated.
295591	ESP sequence number is invalid after lag interface member links down/up.
292057	IKE Certificate config cache is not refreshed after successful certificate renewal through SCEP.
289916	IPSec tunnels with NAT-T stop working after an IKE aggressive mode rekey.
293310	IPSec hardware does not offload properly with dialup tunnels on FortiGate-500D.

Routing

Bug ID	Description
285687	IPv6 multicast route keeps being deleted and re-installed every 210 seconds.

SSLVPN

Bug ID	Description
306020	`sslvpnd` processes leaking FD.
290263	SSLVPN web mode cannot enter text into a Sharepoint application.
300365	SSLVPN stops working when a client is connecting to FG-600C.
294538	Device Detection not working due to virtual MAC.
257689	SSLVPN OWA 2013 send button does not work.
294330	Sharepoint site does not load when using web-mode.

System

Bug ID	Description
301842	When switch port is up during NP6 initialization, it could cause NP6 initialization to stop working.
254979	Incorrect port mapping configuration for 40G port LAG.
292794	CISCO keep alive packets GRE tunnel are not going through FortiGate.
307088	`Internal-switch-mode` switch does not working on FGT/FWF 60D-3G4G-VZW.
295159	USG models cannot register or receive updates when using FMGR as FDS.
296025	A kernel panic occurs if ICMP redirect packet is processed prior to the session being created.
295041	When neighbor MAC changes, IPv6 sessions are not updated with the change.
301574	Leave only one MS VSA in one RADIUS attribute.
258993	Continuous rekey and traffic issues occur when combining `npu-offload` and `keylifekbs` on NP4lite.
293926	Importing software tokens do not work as expected.

Upgrade

Bug ID	Description
304006	Autoupdate schedule time value is lost when upgrading from 5.0.10 to 5.2.5.

WANopt & Webproxy

Bug ID	Description
298777 229886 271526	WAD FD leak issue.
215623	Explicit proxy does not regenerate presented server certificate with deep inspection.
305459	When DLP and the URL filter are enabled, the WAD stops working when the HTTP response is a forwarded request.
293132	Do not offer abbreviated TLS handshake on version mismatch.
289501	Stale connection with Chrome over explicit proxy.

Known Issues

The following issues have been identified in version 5.2.6. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
273910	RTSP/RTP packets may not be forwarded if UTM (IPS and AppCtrl) is enabled. **Note:** This affects FortiGates running IPS engine version below 3.164.

FortiGate 3240C

Bug ID	Description
285520	TCP traffic may not be able to be offloaded in the decryption direction.

FortiGate 3810D

Bug ID	Description
285429	Traffic may not be able to go through the NPU VDOM link with traffic sharper enabled on FortiGate-3810D TP mode.

FortiGate-VM

Bug ID	Description
272438	During the boot-up sequence, the FortiGate-VM device may encounter a harmless configuration error message.

FortiSandbox

Bug ID	Description
269830	The UTM log may incorrectly report a file that has been sent to FortiSandbox. *FortiView* > *FortiSandbox* may still show files are submitted even after the daily upload quota has been reached.
273244	On the FortiGate device in *FortiView* > *FortiSandbox*, the analysis result may show a pending status and the FortiCloud side may show an unknown status.

GUI

Bug ID	Description
267957	The Top Interfering APs chart in the 5G Radio Spectrum Analysis Window may be empty.
268346	*All sessions: filter application*, *threat*, and *threat type*, may not work as expected
271113	When creating an `id_based policy` with SSL enabled, and the set `gui-multipleutm disable` is applied, an *Entry not found* error message may appear.
278638	Explicit policy may be automatically reset to log security events.
285813	When navigating `FortiView > Application` some security action filters may not work.
286226	Users may not be able to create new address objects from the Firewall Policy.
246546	Adding an override application signature may cause all category settings to be lost.
215890	Local-category status display may not change after running `unset category-override` in the CLI.

HA

Bug ID	Description
283697	When a new device joins, the list of devices may not synchronize between master and slave.

System

Bug ID	Description
285981	Adding more than eight members to `LACP get np6_lacp_add_slave` may result in an error.
263864	When the interface is configured with *Auto-Speed*, FG-3240C NP4 Port 1G may stay down after reboot. **Workaround**: Set the interface speed to *1000/Full*.
302272	Medium type may be shown incorrectly on shared ports.
306321	Interface may be mandatory for configuring the GRE tunnel.

VoIP

Bug ID	Description
272278	SIP calls may be denied when using a combination of SIP ALG, IPS, and AppCtrl.

Webfilter

Bug ID	Description
284661	If the requested URL has port number, the URL filter may not block properly.

WiFi

Bug ID	Description
267904	If the client is connecting to an SSID with WPA-Enterprise and User-group, it may not be able to pass the traffic policy.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET

High Performance Network Security